PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-285284

(43)Date of publication of application : 12.10.2001

---

(51)Int.Cl. H04L 9/32

G06F 12/14

G06F 13/00

H04L 12/28

H04L 12/22

---

(21)Application number : 2000-094851 (71)Applicant : TOSHIBA CORP

(22)Date of filing : 30.03.2000 (72)Inventor : SAITO TAKESHI

---

(54) TRANSMITTER AND ITS TRANSMISSION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a transmitter that can transmit literary works to a receiver while taking the copyright protection into account by performing authentication/ key exchange only with the receiver in existence on a local network and to provide its transmission method.

SOLUTION: The transmitter 10 is connected to the local network 12. This transmitter 10 consists of a transmission section 24 that transmits encrypted data including literary works such as movies and music data to a receiver 18a, a local communication discrimination section 22 that discriminates whether or not the receiver 18a is connected to the local network 12, and an authentication/key exchange section 20 that performs authentication/key exchange with the receiver 18a only when the discrimination section 22 discriminates that the receiver 18a is connected to the local network 12.

LEGAL STATUS [Date of request for examination] 20.09.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3749817

[Date of registration] 09.12.2005

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] The transmitting section which is the sending set which is connected to the local network which can connect only a specific terminal, and transmits the enciphered data to a receiving set, and transmits encryption data to this receiving set, The sending set characterized by having the decision section which judges whether said receiving set is connected to said local network, and the authentication and the key exchange section which perform authentication and key exchange between said receiving sets only when it is judged that it connects with said local network.

[Claim 2] Said authentication and key exchange section are a sending set according to claim 1 characterized by what the authentication and the key

exchange demand from said receiving set are refused for when it is judged that said receiving set is not connected to said local network.

[Claim 3] Said decision section is a sending set according to claim 1 characterized by what it has a means to detect whether both said sending set and a receiving set exist on the same address assigned to said local network for.

[Claim 4] Said detection means is a sending set according to claim 3 characterized by what it has a means to collate whether the subnet ID of the packet sent from said receiving set is in agreement with the subnet ID of said sending set for.

[Claim 5] Said decision section is a sending set according to claim 1 characterized by what it has a means to detect whether both said sending set and a receiving set exist in the same local scope for using the scope field of the packet sent from said receiving set.

[Claim 6] The packet sent from said receiving set is a sending set according to claim 4 or 5 characterized by what is been the packet which constitutes the data Request to Send, or the authentication and the key exchange demand to said sending set from said receiving set.

[Claim 7] The process which is the transmitting approach of transmitting the data enciphered from the sending set connected to the local network which can connect only a specific terminal to a receiving set, and receives the data

Request to Send from this receiving set, The process which transmits encryption data to said receiving set based on this data Request to Send, The process which receives the authentication demand from said receiving set, the process which judges whether said receiving set is connected to said local network, and only when it is judged that said receiving set is connected to said local network, between said receiving sets The transmitting approach characterized by including the process which performs authentication and key exchange.

[Claim 8] Said decision process is the transmitting approach according to claim 7 characterized by what the step which detects whether said receiving set exists on the address assigned to said local network is included for.

[Claim 9] Said decision process is the transmitting approach according to claim 7 characterized by what the step which detects whether said receiving set exists in the same local scope as a sending set is included for.

[Claim 10] The transmitting approach according to claim 7 characterized by what the process which transmits the notice of authentication disapproval at said receiving set is further included for only when it is judged that said receiving set is not connected to said local network after said decision process.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the sending set equipped with the function to realize protection of copyrights, and its transmitting approach.

[0002]

[Description of the Prior Art] The goods called digital information appliances have been increasing with progress of digitization and a network in recent years. Digital information appliances are goods groups from which spread is expected with initiation of digital broadcasting. Goods treating a digital data digital content, such as television corresponding to digital broadcasting, and a set top box, digital VTR, a DVD player, a hard disk recorder, are widely contained in these digital information appliances.

[0003] In case such digital information appliances are used, protection ** by the copyright of a work is mentioned as one of the matters which should be taken

into consideration. digital data is easy to copy illegally while an advantage, like there is no quality degradation at the time of a copy is emphasized -- etc. -- it is because it has a fault. For example, IEEE1394 which is the digital network which connects digital AV equipments is equipped with authentication and a key exchange style, and the function of data encryption for prevention of literary piracy.

[0004] Here, the case where AV data which need protection of copyrights are transmitted to a receiving set from a sending set is considered. In this transfer, the point which should be careful of is a point that it is the premise of protection of copyrights to exchange required AV data of protection of copyrights within limits which an individual or a family enjoys. And an exchange of AV data between others is the point that it should not be carried out, unless payment of an audience fee, a royalty, etc. follows.

[0005]

[Problem(s) to be Solved by the Invention] Although it is thought that the class of digital network will increase in the future [near] to wireless and various classes, such as a personal computer network, the present condition is that protection of copyrights is not yet taken into consideration about these many.

[0006] Moreover, as there is a network broadly and it was explained above from the local thing to the global thing, from a viewpoint of protection of copyrights,

the need has distinguished clearly.

[0007] This invention solves such a technical problem, is checking whether a receiving set existing in a local screen oversize, and aims at offering the receiving set which exists in a local screen oversize, the sending set which can perform authentication and key exchange, and its transmitting approach.

[0008]

[Means for Solving the Problem] The transmitting section which this invention is connected to the local network which can connect only a specific terminal, and is the sending set which transmits the enciphered data to a receiving set, and transmits encryption data to a receiving set in order to solve the above-mentioned technical problem, the decision section which judges whether the receiving set is connected to the local network, and the authentication and the key exchange section which perform authentication and key exchange only between the receiving sets judged to connect with a local network -- since -- it is characterized [1st] by being the sending set constituted. Here, a "local network" is a network with which an exchange of the data between an individual's within the limits or a family is performed, for example, is home networks, such as IEEE1394.

[0009] In the 1st description of this invention, the exchange of data which should perform protection of copyrights is permitted by considering that only the

communication link closed within the net [this / local] is the communication link for enjoying oneself between an individual or a family. And since it cannot consider that the communication link which is not closed with this local network is the communication link for enjoying oneself between an individual or a family, the exchange of data which should perform protection of copyrights is not permitted. For this reason, the receiving set which requires data playback judges beforehand whether it exists in a local screen oversize, and the exchange of data in consideration of protection of copyrights of it is attained by performing authentication and key exchange with a receiving set based on that decision result. Namely, only the receiving set connected to the local network performs authentication and key exchange, and, thereby, can decode the enciphered data now.

[0010] The 2nd description of this invention starts the transmitting approach which the sending set stated in the 1st above-mentioned description realizes. The process which is the transmitting approach of transmitting the data enciphered from the sending set connected to the local network which can connect only a specific terminal to a receiving set, and receives the data Request to Send from the receiving set, The process which transmits encryption data to a receiving set based on the data Request to Send, The process which receives the authentication demand from a receiving set, the process which

judges whether the receiving set is connected to the local network, and only when it is judged that the receiving set is connected to a local network, between receiving sets It is the transmitting approach which includes at least the process which performs authentication and key exchange.

[0011]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail with reference to a drawing. In the publication of the following drawings, the same or similar sign is given to the same or similar part.

[0012] Drawing 1 is a block diagram with which the sending set concerning the gestalt of operation of this invention has been arranged and in which showing the whole network-system configuration. As shown in drawing 1 , the sending set 10 concerning the gestalt of operation of this invention is connected to the local networks 12, such as Ethernet (trademark). And a router 14 is connected to the local network 12, and the local network 10 and the Internet 16 are connected by the router 14. Receiving set 18a will be connected to the local network 12, receiving set 18b will be connected to the Internet 16, and both receiving sets 18a and 18b tend to receive AV data transmitted from a sending set 10. As AV data, a text, a photograph and an illustration, pictures, animation, a movie, music, voice, a TV program, WWW data, etc. are mentioned. Here, in order to attain simplification of explanation, a work is contained in some AV data, or suppose

that the AV data itself are a work.

[0013] Here, the case where required AV data of protection of copyrights are transmitted to receiving sets 18a and 18b from a sending set 10 is considered. In this case, as explanation of a Prior art also described the point which should be careful of, within an individual or limits which it gives a broad interpretation of and which a family enjoys, it is the premise of protection of copyrights to exchange AV data, unless payment of an audience fee or a royalty follows, I hear that an exchange of AV data between others should not be performed but, and there is. For example, as an exchange of the data between others, the open communication link through public networks, such as the Internet and a telephone network, is mentioned, and the communication link closed to home networks, such as IEEE1394, is mentioned as an example of a type of an exchange of the data between the homes within the limits of an individual.

[0014] Then, in order to perform protection of copyrights, the following two regulations are used about AV data transfer in the network system of drawing 1 .

[0015] (A) The communication link closed on the local network 12 permits the exchange of AV data which should perform protection of copyrights.

[0016] (B) The communication link which is not closed with the local network 12 does not permit the exchange of AV data which should perform protection of copyrights.

[0017] It is because it can be regarded as the communication link for enjoying the communication link which closed the regulation of the above (A) with the local network 12 between an individual or a home here, and is because it cannot usually consider that the communication link which does not close the regulation of the above (B) with the local network 12 is the communication link for enjoying oneself between an individual or a home.

[0018] Drawing 2 is the block diagram showing the configuration of the sending set concerning the gestalt of operation of this invention. As shown in drawing 2 , the sending set 10 concerning the gestalt of this operation The authentication and the key message-exchange section 20 which performs the authentication and the key message exchange between receiving sets 18 (18a, 18b), The local communication link decision section 22 which judges to any of the regulation of the above-mentioned (A) and (B) the communication link with the receiving set 18 which requires authentication and the key message exchange corresponds, the transmitting section 24 which transmits enciphered AV data to a receiving set 18, and the network interface 26 used as an interface with the local network 12 -- since -- it is constituted. Although the local communication link decision section 22 is arranged in authentication and the key message-exchange section 20, of course, drawing 2 is available for it, even if arranged out of authentication and the key message-exchange section 20.

[0019] Next, with reference to drawing 3 thru/or drawing 5 , actuation of the sending set concerning the gestalt of operation of this invention is explained. Drawing 3 is a processing sequence chart between the sending set 10 concerning the gestalt of operation of this invention, receiving set 18a connected to the local network 12, and **, drawing 4 is a processing sequence chart between the sending set 10 concerning the gestalt of operation of this invention, receiving set 18b connected to the Internet 16, and **, and drawing 5 is a flow chart which shows the procedure of the transmitting approach of the sending set 10 concerning the gestalt of operation of this invention.

[0020] (b) In step S101 of communication link (1) drawing 3 between a sending set 10 and receiving set 18a, receiving set 18a requires playback of AV data from a sending set 10 through the local network 12 (step S301 of drawing 5). The playback demand of AV data is performed by being publishing the command of a playback demand for example, using an audio-visual control (AV/C) command.

[0021] (2) In step S102 of drawing 3 , the sending set 10 which received the Request to Send of AV data transmits AV data enciphered with the encryption key K1 to receiving set 18a through the local network 12 for protection of copyrights (step S302 of drawing 5).

[0022] (3) In step S103 of drawing 3 , receiving set 18a which received

enciphered AV data requires authentication and key exchange from a sending set 10 (step S303 of drawing 5).

[0023] (4) In step S104 of drawing 3 , the sending set 10 which received authentication and a key exchange demand judges whether receiving set 18a exists on the local network 12 based on the packet of its authentication and key exchange demand (step S304 of drawing 5). The following two are mentioned as criteria it can be judged that exist on the local network 12.

[0024] (C) The source address ID of authentication and a key exchange demand packet, i.e., the subnet of address ** of receiving set 18a, be in agreement with the subnet ID of sending set 10 self.

[0025] (D) The scope field of an IPv6 packet should show the local scope.

[0026] In addition, even if it performs this decision based on the packet of the playback demand from receiving set 18a, of course, it is not cared about. When an alteration etc. is made during the transfer, it becomes impossible moreover, for the packet of these playback demand and the packet of authentication and a key exchange demand to perform exact decision. For this reason, the signature for alteration detection etc. should be performed to the value of the source address of each packet, and each scope field.

[0027] (5) Since receiving set 18a exists on the local network 12 (step S304YES of drawing 5), in step S105 of drawing 3 , a sending set 10 performs

authentication and key exchange between receiving set 18a (step S306 of drawing 5). By this authentication and key exchange, receiving set 18a receives a decode key required for decode of encryption AV data. For example, if the code technique used is a common key encryptosystem, the decode key is the same as the encryption key K1.

[0028] (6) In step S106 of drawing 3 , receiving set 18a which received the decode key K1 decodes AV data received previously.

[0029] (b) In step S201 of communication link (1) drawing 4 between a sending set 10 and receiving set 18b, receiving set 18b requires playback of AV data from a sending set 10 through the Internet 16, a router 14, and the local network 12 (step S301 of drawing 5). The playback demand of AV data is performed by being publishing the command of a playback demand like the case where it is the above-mentioned (**), for example, using an audio-visual control (AV/C) command.

[0030] (2) In step S202 of drawing 4 , the sending set 10 which received the Request to Send of AV data transmits AV data enciphered with the encryption key K1 to receiving set 18b through the local network 12, a router 14, and the Internet 16 for protection of copyrights (step S302 of drawing 5).

[0031] (3) In step S203 of drawing 4 , receiving set 18b which received enciphered AV data requires authentication and key exchange from a sending

set 10 (step S303 of drawing 5).

[0032] (4) In step S204 of drawing 4 , the sending set 10 which received authentication and a key exchange demand judges whether receiving set 10b exists on the local network 12 based on the packet of its authentication and key exchange demand (step S304 of drawing 5).

[0033] (5) Since receiving set 18b does not exist on the local network 12 (step S304NO of drawing 5), in step S205 of drawing 4 , a sending set 10 notifies authentication disapproval to receiving set 18b (step S305 of drawing 5). By this authentication disapproval, receiving set 18b cannot obtain a decode key required in order to decode AV data received previously. For this reason, receiving set 18b which does not exist on the local network 12 becomes possible [preventing] about AV data coming to hand unjustly.

[0034] Thus, according to the gestalt of operation of this invention, it becomes possible to transmit required AV data of protection of copyrights only to the receiving set which exists in a local screen oversize. For this reason, it becomes possible to protect appropriately the work transmitted on the network which is increasing steadily with digitization and a network in recent years, and that importance is very high.

[0035]

[Effect of the Invention] According to this invention, the receiving set which exists

in a local screen oversize, and the sending set which performs authentication and key exchange are realizable by checking whether a receiving set exists in a local screen oversize.

[0036] According to this invention, the receiving set which exists in a local screen oversize, and the transmitting approach of performing authentication and key exchange are realizable by checking whether a receiving set exists in a local screen oversize.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram with which the sending set concerning the

gestalt of operation of this invention has been arranged and in which showing the whole network-system configuration.

[Drawing 2] It is the block diagram showing the concrete configuration of the sending set concerning the gestalt of operation of this invention.

[Drawing 3] It is a processing sequence chart between the sending set concerning the gestalt of operation of this invention, and a receiving set.

[Drawing 4] It is a processing sequence chart between the sending set concerning the gestalt of operation of this invention, and a receiving set.

[Drawing 5] It is the flow chart which shows the procedure of the transmitting approach of the sending set concerning the gestalt of operation of this invention.

[Description of Notations]

10 Sending Set

12 Local Network

14 Router

16 Internet

18 Receiving Set

20 Authentication and Key Message-Exchange Section

22 Local Communication Link Decision Section

24 Transmitting Section

26 Network Interface

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－285284
（P2001－285284A）
(43)公開日　平成13年10月12日(2001.10.12)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)	
Ｈ０４Ｌ	9/32		Ｇ０６Ｆ	12/14	３２０Ａ	５Ｂ０１７
Ｇ０６Ｆ	12/14	３２０		13/00	５４０Ｓ	５Ｊ１０４
	13/00	５４０	Ｈ０４Ｌ	9/00	６７３Ｂ	５Ｋ０３０
Ｈ０４Ｌ	12/28			11/00	３１０Ｚ	５Ｋ０３３
	12/22			11/26		

審査請求　未請求　請求項の数10　ＯＬ　（全 ６ 頁）

(21)出願番号　特願2000－94851(P2000－94851)

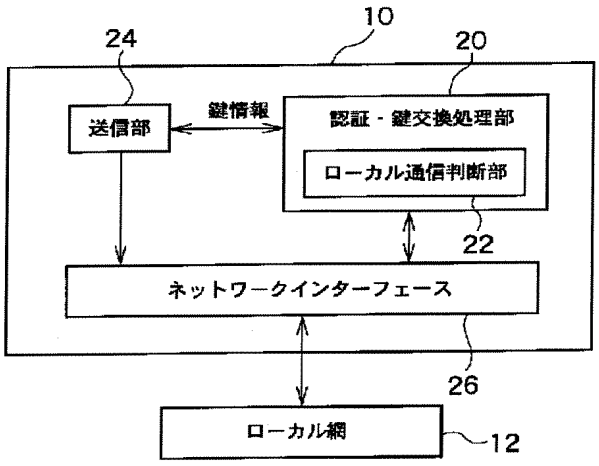
(22)出願日　平成12年３月30日(2000.3.30)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　斉藤　健
神奈川県川崎市幸区小向東芝町１　株式会社東芝研究開発センター内
(74)代理人　100083806
弁理士　三好　秀和　（外７名）

最終頁に続く

(54)【発明の名称】　送信装置およびその送信方法

(57)【要約】
【課題】　ローカル網上に存在する受信装置のみと認証・鍵交換を実行することで、著作権保護を考慮して著作物を受信装置に送信できる送信装置、およびその送信方法を提供する。
【解決手段】　ローカル網１２に接続された送信装置１０である。この送信装置１０は、受信装置１８ａに、暗号化された、映画、音楽等の著作物を含むデータを送信する送信部２４と、受信装置１８ａがローカル網１２に接続されているか否かを判断するローカル通信判断部２２と、ローカル網１２に接続されていると判断された場合のみ、受信装置１８ａとの間で、認証・鍵交換を実行する認証・鍵交換部２０と、から構成される。



【特許請求の範囲】
【請求項１】　特定の端末のみが接続可能なローカル網に接続され、暗号化されたデータを受信装置に送信する送信装置であって、
該受信装置に暗号化データを送信する送信部と、
前記受信装置が前記ローカル網に接続されているか否かを判断する判断部と、
前記ローカル網に接続されていると判断された場合のみ、前記受信装置との間で、認証・鍵交換を実行する認証・鍵交換部とを有することを特徴とする送信装置。
【請求項２】　前記認証・鍵交換部は、前記受信装置が前記ローカル網に接続されていないと判断した場合には、前記受信装置からの認証・鍵交換要求を拒絶する、ことを特徴とする請求項１に記載の送信装置。
【請求項３】　前記判断部は、前記送信装置および受信装置の両方が、前記ローカル網に割り当てられた同一のアドレス上に存在するか否かを検知する手段、を備える、ことを特徴とする請求項１に記載の送信装置。
【請求項４】　前記検知手段は、前記受信装置から送られたパケットのサブネットIDが前記送信装置のサブネットIDと一致するか否かを照合する手段、を備える、ことを特徴とする請求項３に記載の送信装置。
【請求項５】　前記判断部は、前記受信装置から送られるパケットのスコープフィールドを用いて、前記送信装置および受信装置の両方が、同一のローカルスコープ内に存在するか否かを検知する手段を備える、ことを特徴とする請求項１に記載の送信装置。
【請求項６】　前記受信装置から送られるパケットは、前記受信装置からの、前記送信装置に対するデータ送信要求または認証・鍵交換要求を構成するパケットである、ことを特徴とする請求項４または５に記載の送信装置。
【請求項７】　特定の端末のみが接続可能なローカル網に接続された送信装置から暗号化されたデータを受信装置に送信する送信方法であって、
該受信装置からのデータ送信要求を受け取る工程と、
該データ送信要求に基づき、前記受信装置に暗号化データを送信する工程と、
前記受信装置からの認証要求を受け取る工程と、
前記受信装置が前記ローカル網に接続されているか否かを判断する工程と、
前記受信装置が前記ローカル網に接続されていると判断された場合のみ、前記受信装置との間で、認証・鍵交換を実行する工程とを含むことを特徴とする送信方法。
【請求項８】　前記判断工程は、前記受信装置が、前記ローカル網に割り当てられたアドレス上に存在するか否かを検知するステップ、を含む、ことを特徴とする請求項７に記載の送信方法。
【請求項９】　前記判断工程は、前記受信装置が、送信装置と同一のローカルスコープ内に存在するか否かを検知するステップ、を含む、ことを特徴とする請求項７に記載の送信方法。
【請求項１０】　前記判断工程の後に、前記受信装置が前記ローカル網に接続されていないと判断された場合のみ、前記受信装置に認証不許可通知を送信する工程を、さらに含む、ことを特徴とする請求項７に記載の送信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、著作権保護を実現する機能を備えた送信装置およびその送信方法に関する。
【０００２】
【従来の技術】近年の、デジタル化・ネットワーク化の進展に伴って、デジタル情報家電と呼ばれる商品が増加して来ている。デジタル情報家電は、デジタル放送の開始に伴い、普及が期待される商品群である。このデジタル情報家電には、デジタル放送対応テレビや、セットトップボックス、デジタルVTR、DVDプレーヤ、ハードディスクレコーダ等、デジタルデータ・デジタルコンテンツを扱う商品が広く含まれる。
【０００３】このようなデジタル情報家電を利用する際に、考慮すべき事柄の一つとして、著作物の著作権による保護、が挙げられる。デジタルデータは、コピー時の品質劣化がない等の利点が強調される反面、不正コピーが容易である等の欠点を持っているためである。たとえばデジタルAV機器どうしを接続するデジタルネットワークであるIEEE1394には、著作権侵害の防止のため、認証・鍵交換機構や、データ暗号化の機能が備えられる。
【０００４】ここで、著作権保護が必要なAVデータを、送信装置から受信装置に転送する場合を考える。この転送において、注意すべき点は、個人あるいは家族の楽しむ範囲内で、著作権保護の必要なAVデータのやり取りを行なうことが、著作権保護の前提である点である。そして、他人との間でのAVデータのやり取りは、視聴料や著作権料等の支払いが伴わない限り、行われるべきではないという点である。
【０００５】
【発明が解決しようとする課題】近い将来、デジタルネットワークの種類は、無線や、パソコンネットワーク等、いろいろな種類に増加するものと考えられるが、これらの多くについては、未だ著作権保護が考慮されていないのが現状である。
【０００６】また、ネットワークはローカルなものからグローバルなものまで幅広くあり、上記で説明したように、著作権保護の観点からは、明確に区別することが必要がある。
【０００７】本発明は、このような課題を解決し、受信装置がローカル網上に存在するか否かを確認することで、ローカル網上に存在する受信装置のみと認証・鍵交

換を実行できる送信装置、およびその送信方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記課題を解決するため、本発明は、特定の端末のみが接続可能なローカル網に接続され、暗号化されたデータを受信装置に送信する送信装置であり、受信装置に暗号化データを送信する送信部と、受信装置がローカル網に接続されているか否かを判断する判断部と、ローカル網に接続されていると判断された受信装置のみとの間で、認証・鍵交換を実行する認証・鍵交換部と、から構成される送信装置であることを第１の特徴とする。ここで、「ローカル網」とは、個人の範囲内、あるいは家族間でのデータのやりとりが行なわれる網であり、たとえばIEEE1394等のホームネットワークである。

【０００９】本発明の第１の特徴では、このローカル網内に閉じた通信のみを、個人あるいは家族間で楽しむための通信とみなすことで、著作権保護を行なうべきデータのやりとりを許容する。そして、このローカル網で閉じない通信は、個人あるいは家族間で楽しむための通信とみなすことができないため、著作権保護を行なうべきデータのやりとりを許容しない。このため、データ再生を要求する受信装置がローカル網上に存在するか否かをあらかじめ判断し、その判断結果に基づいて、受信装置と認証・鍵交換を実行することで、著作権保護を考慮したデータのやりとりが可能となる。すなわち、ローカル網に接続された受信装置のみが、認証・鍵交換を実行し、それにより、暗号化されたデータを復号できるようになる。

【００１０】本発明の第２の特徴は、上記の第１の特徴で述べた送信装置が実現する送信方法に係り、特定の端末のみが接続可能なローカル網に接続された送信装置から暗号化されたデータを受信装置に送信する送信方法であって、その受信装置からのデータ送信要求を受け取る工程と、そのデータ送信要求に基づき、受信装置に暗号化データを送信する工程と、受信装置からの認証要求を受け取る工程と、受信装置がローカル網に接続されているか否かを判断する工程と、受信装置がローカル網に接続されていると判断された場合のみ、受信装置との間で、認証・鍵交換を実行する工程と、を少なくとも含む送信方法であることである。

【００１１】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について詳細に説明する。以下の図面の記載において、同一または類似の部分には同一または類似の符号を付している。

【００１２】図１は、本発明の実施の形態に係る送信装置が配置された、ネットワーク・システムの全体構成を示すブロック図である。図１に示すように、本発明の実施の形態に係る送信装置１０は、イーサネット（登録商標）等のローカル網１２に接続される。そして、ローカル網１２にルータ１４が接続され、ルータ１４によって、ローカル網１０とインターネット１６とが接続される。ローカル網１２には受信装置１８ａが接続され、インターネット１６には受信装置１８ｂが接続され、受信装置１８ａおよび１８ｂの両方が、送信装置１０から送信されるAVデータを受信しようとすることになる。AVデータとしてはたとえば、テキストや、写真、イラスト、絵画、アニメ、映画、音楽、音声、テレビ番組、WWWデータ等が挙げられる。ここでは、説明の簡単化を図るため、AVデータの一部に著作物が含まれる、あるいはAVデータ自体が著作物であるとする。

【００１３】ここで、送信装置１０から受信装置１８ａおよび１８ｂに、著作権保護の必要なAVデータを転送する場合を考える。この場合、注意すべき点は、従来の技術の説明でも述べたように、個人、あるいは拡大解釈して家族の楽しむ範囲内で、AVデータのやりとりを行なうことが著作権保護の前提であり、他人との間のAVデータのやりとりは、視聴料や著作権料の支払いが伴わない限り、行なわれるべきではないということである。たとえば他人との間でのデータのやりとりとしては、インターネットや電話網等の公衆網を介したオープンな通信が挙げられ、個人の範囲内、あるいは家庭間のデータのやりとりの典型例として、IEEE1394等のホームネットワークに閉じた通信が挙げられる。

【００１４】そこで、著作権保護を行なうため、図１のネットワーク・システムにおけるAVデータの転送に関し、次の２つの規則を用いる。

【００１５】（Ａ）ローカル網１２に閉じた通信は、著作権保護を行なうべきAVデータのやりとりを許容する。

【００１６】（Ｂ）ローカル網１２で閉じない通信は、著作権保護を行なうべきAVデータのやりとりを許容しない。

【００１７】ここで、上記（Ａ）の規則は、ローカル網１２で閉じた通信は、個人あるいは家庭間で楽しむための通信と見なすことができるからであり、上記（Ｂ）の規則は、ローカル網１２で閉じない通信は、個人あるいは家庭間で楽しむための通信と、通常、見なすことができないからである。

【００１８】図２は、本発明の実施の形態に係る送信装置の構成を示すブロック図である。図２に示すように、この実施の形態に係る送信装置１０は、受信装置１８（１８ａ，１８ｂ）との間での認証・鍵交換処理を実行する認証・鍵交換処理部２０と、認証・鍵交換処理を要求する受信装置１８との通信が、上記の（Ａ）および（Ｂ）の規則のいずれに該当するかを判断するローカル通信判断部２２と、暗号化されたAVデータを受信装置１８に送信する送信部２４と、ローカル網１２とのインターフェースとなるネットワークインターフェース２６と、から構成される。図２では、ローカル通信判断部２

２は、認証・鍵交換処理部２０内に配置されているが、もちろん、認証・鍵交換処理部２０外に配置されてももちろん構わない。

【００１９】次に、図３ないし図５を参照して、本発明の実施の形態に係る送信装置の動作について説明する。図３は、本発明の実施の形態に係る送信装置１０と、ローカル網１２に接続された受信装置１８ａと、の間の処理シーケンスチャートであり、図４は、本発明の実施の形態に係る送信装置１０と、インターネット１６に接続された受信装置１８ｂと、の間の処理シーケンスチャートであり、図５は、本発明の実施の形態に係る送信装置１０の送信方法の処理手順を示すフローチャートである。

【００２０】（イ）送信装置１０と受信装置１８ａとの間の通信

（１）図３のステップＳ１０１において、受信装置１８ａが、ローカル網１２を介して、送信装置１０に対して、AVデータの再生を要求する（図５のステップＳ３０１）。AVデータの再生要求は、たとえばオーディオ・ビジュアル・コントロール（AV/C）コマンドを用いて、再生要求のコマンドを発行することで、行われる。

【００２１】（２）図３のステップＳ１０２において、AVデータの送信要求を受けた送信装置１０は、著作権保護のため、暗号化鍵K1で暗号化されたAVデータを、ローカル網１２を介して、受信装置１８ａに送信する（図５のステップＳ３０２）。

【００２２】（３）図３のステップＳ１０３において、暗号化されたAVデータを受信した受信装置１８ａは、送信装置１０に対して、認証・鍵交換を要求する（図５のステップＳ３０３）。

【００２３】（４）図３のステップＳ１０４において、認証・鍵交換要求を受けた送信装置１０は、その認証・鍵交換要求のパケットに基づいて、受信装置１８ａがローカル網１２上に存在するか否かを判断する（図５のステップＳ３０４）。ローカル網１２上に存在すると判断できる基準として、たとえば次の２つが挙げられる。

【００２４】（C）認証・鍵交換要求パケットのソースアドレス、すなわち受信装置１８ａのアドレス、のサブネットIDが、送信装置１０自身のサブネットIDと一致すること。

【００２５】（D）IPv6パケットのスコープフィールドがローカルスコープを示していること。

【００２６】なお、この判断は、受信装置１８ａからの再生要求のパケットに基づいて、実行しても、もちろん構わない。また、これら再生要求のパケットおよび認証・鍵交換要求のパケットは、その転送中に、改ざん等がなされてしまうと、正確な判断を行なうことができなくなる。このため、各パケットのソースアドレスおよびスコープフィールドそれぞれの値に、改ざん検出のための署名等を施すべきである。

【００２７】（５）受信装置１８ａはローカル網１２上に存在するので（図５のステップＳ３０４ＹＥＳ）、図３のステップＳ１０５において、送信装置１０は、受信装置１８ａとの間で、認証・鍵交換を実行する（図５のステップＳ３０６）。この認証・鍵交換によって、受信装置１８ａは、暗号化ＡＶデータの復号のために必要な復号鍵を入手する。たとえば、利用される暗号技術が共通鍵暗号であれば、復号鍵は暗号化鍵K1と同一である。

【００２８】（６）図３のステップＳ１０６において、復号鍵K1を入手した受信装置１８ａは、先に受信したAVデータを復号する。

【００２９】（ロ）送信装置１０と受信装置１８ｂとの間の通信

（１）図４のステップＳ２０１において、受信装置１８ｂが、インターネット１６、ルータ１４およびローカル網１２、を介して、送信装置１０に対して、AVデータの再生を要求する（図５のステップＳ３０１）。上記（イ）の場合と同様、AVデータの再生要求は、たとえばオーディオ・ビジュアル・コントロール（AV/C）コマンドを用いて、再生要求のコマンドを発行することで、行われる。

【００３０】（２）図４のステップＳ２０２において、AVデータの送信要求を受けた送信装置１０は、著作権保護のため、暗号化鍵K1で暗号化されたAVデータを、ローカル網１２、ルータ１４およびインタネット１６を介して、受信装置１８ｂに送信する（図５のステップＳ３０２）。

【００３１】（３）図４のステップＳ２０３において、暗号化されたAVデータを受信した受信装置１８ｂは、送信装置１０に対して、認証・鍵交換を要求する（図５のステップＳ３０３）。

【００３２】（４）図４のステップＳ２０４において、認証・鍵交換要求を受けた送信装置１０は、その認証・鍵交換要求のパケットに基づいて、受信装置１０ｂがローカル網１２上に存在するか否かを判断する（図５のステップＳ３０４）。

【００３３】（５）受信装置１８ｂはローカル網１２上に存在しないので（図５のステップＳ３０４ＮＯ）、図４のステップＳ２０５において、送信装置１０は、受信装置１８ｂに対して、認証不許可を通知する（図５のステップＳ３０５）。この認証不許可によって、受信装置１８ｂは、先に受信したAVデータを復号するために必要な復号鍵を入手することができない。このため、ローカル網１２上に存在しない受信装置１８ｂが、不正にAVデータを入手することを、未然に防ぐことが可能となる。

【００３４】このように、本発明の実施の形態によれば、ローカル網上に存在する受信装置のみに対して、著作権保護の必要なAVデータを送信することが可能となる。このため、近年のデジタル化・ネットワーク化に伴って増加する一方である、ネットワーク上で送信される

著作物を適切に保護することが可能となり、その重要性はきわめて高いものである。

【００３５】

【発明の効果】本発明によれば、受信装置がローカル網上に存在するか否かを確認することで、ローカル網上に存在する受信装置のみと認証・鍵交換を実行する送信装置を実現できる。

【００３６】本発明によれば、受信装置がローカル網上に存在するか否かを確認することで、ローカル網上に存在する受信装置のみと認証・鍵交換を実行する送信方法を実現できる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る送信装置が配置された、ネットワーク・システムの全体構成を示すブロック図である。

【図２】本発明の実施の形態に係る送信装置の具体的な構成を示すブロック図である。

【図３】本発明の実施の形態に係る送信装置と受信装置間の処理シーケンスチャートである。

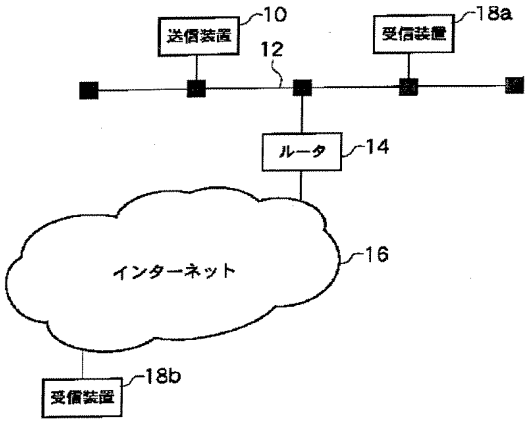
【図４】本発明の実施の形態に係る送信装置と受信装置間の処理シーケンスチャートである。

【図５】本発明の実施の形態に係る送信装置の送信方法の処理手順を示すフローチャートである。

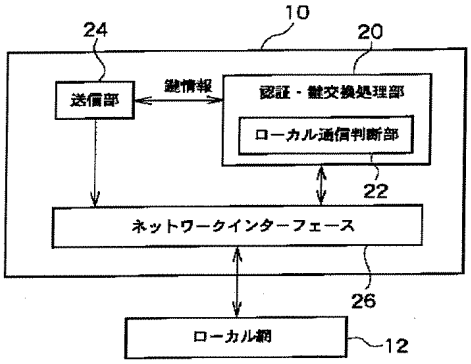
【符号の説明】

１０　送信装置
１２　ローカル網
１４　ルータ
１６　インターネット
１８　受信装置
２０　認証・鍵交換処理部
２２　ローカル通信判断部
２４　送信部
２６　ネットワークインターフェース

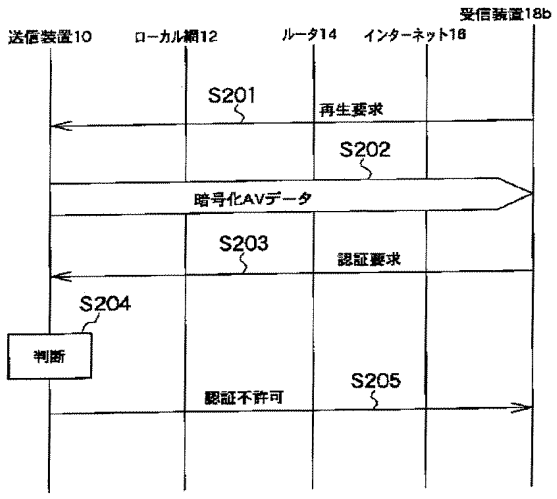
【図１】



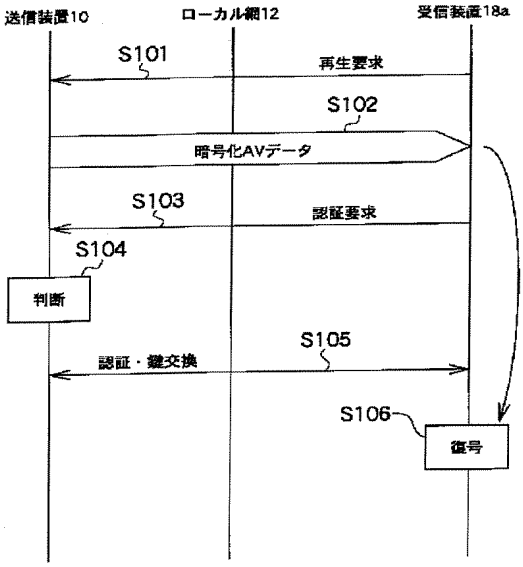
【図２】



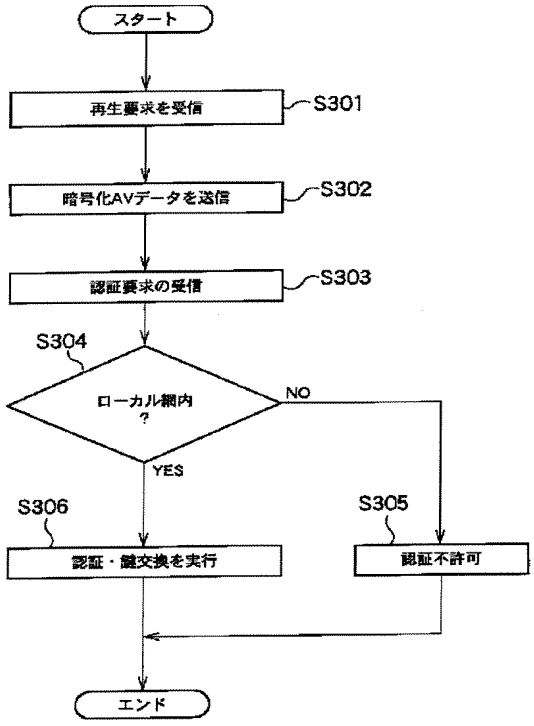
【図４】



【図３】



【図５】



フロントページの続き

Ｆターム(参考) 5B017 AA03 BA05 BA07 CA16
5J104 AA07 AA12 AA16 EA04 EA15
KA02 PA07
5K030 GA15 HA08 HB21 HC14 JL09
JT04 LD20
5K033 AA08 BA01 BA15 CB01 DA01
DA13

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－285284
（P2001－285284A）
(43)公開日　平成13年10月12日(2001.10.12)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ	9/32		Ｇ０６Ｆ	12/14	３２０Ａ　５Ｂ０１７
Ｇ０６Ｆ	12/14	３２０		13/00	５４０Ｓ　５Ｊ１０４
	13/00	５４０	Ｈ０４Ｌ	9/00	６７３Ｂ　５Ｋ０３０
Ｈ０４Ｌ	12/28			11/00	３１０Ｚ　５Ｋ０３３
	12/22			11/26	

審査請求　未請求　請求項の数10　ＯＬ　（全 6 頁）

(21)出願番号　特願2000－94851(P2000－94851)

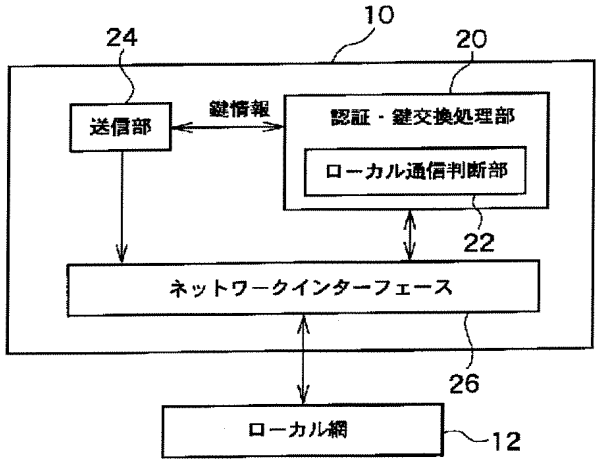
(22)出願日　平成12年３月30日(2000.3.30)

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　斉藤　健
神奈川県川崎市幸区小向東芝町１　株式会社東芝研究開発センター内
(74)代理人　100083806
弁理士　三好　秀和　（外７名）

最終頁に続く

(54)【発明の名称】　送信装置およびその送信方法

(57)【要約】
【課題】　ローカル網上に存在する受信装置のみと認証・鍵交換を実行することで、著作権保護を考慮して著作物を受信装置に送信できる送信装置、およびその送信方法を提供する。
【解決手段】　ローカル網１２に接続された送信装置１０である。この送信装置１０は、受信装置１８ａに、暗号化された、映画、音楽等の著作物を含むデータを送信する送信部２４と、受信装置１８ａがローカル網１２に接続されているか否かを判断するローカル通信判断部２２と、ローカル網１２に接続されていると判断された場合のみ、受信装置１８ａとの間で、認証・鍵交換を実行する認証・鍵交換部２０と、から構成される。



【特許請求の範囲】
【請求項１】　特定の端末のみが接続可能なローカル網に接続され、暗号化されたデータを受信装置に送信する送信装置であって、
該受信装置に暗号化データを送信する送信部と、
前記受信装置が前記ローカル網に接続されているか否かを判断する判断部と、
前記ローカル網に接続されていると判断された場合のみ、前記受信装置との間で、認証・鍵交換を実行する認証・鍵交換部とを有することを特徴とする送信装置。
【請求項２】　前記認証・鍵交換部は、前記受信装置が前記ローカル網に接続されていないと判断した場合には、前記受信装置からの認証・鍵交換要求を拒絶する、ことを特徴とする請求項１に記載の送信装置。
【請求項３】　前記判断部は、前記送信装置および受信装置の両方が、前記ローカル網に割り当てられた同一のアドレス上に存在するか否かを検知する手段、を備える、ことを特徴とする請求項１に記載の送信装置。
【請求項４】　前記検知手段は、前記受信装置から送られたパケットのサブネットIDが前記送信装置のサブネットIDと一致するか否かを照合する手段、を備える、ことを特徴とする請求項３に記載の送信装置。
【請求項５】　前記判断部は、前記受信装置から送られるパケットのスコープフィールドを用いて、前記送信装置および受信装置の両方が、同一のローカルスコープ内に存在するか否かを検知する手段を備える、ことを特徴とする請求項１に記載の送信装置。
【請求項６】　前記受信装置から送られるパケットは、前記受信装置からの、前記送信装置に対するデータ送信要求または認証・鍵交換要求を構成するパケットである、ことを特徴とする請求項４または５に記載の送信装置。
【請求項７】　特定の端末のみが接続可能なローカル網に接続された送信装置から暗号化されたデータを受信装置に送信する送信方法であって、
該受信装置からのデータ送信要求を受け取る工程と、
該データ送信要求に基づき、前記受信装置に暗号化データを送信する工程と、
前記受信装置からの認証要求を受け取る工程と、
前記受信装置が前記ローカル網に接続されているか否かを判断する工程と、
前記受信装置が前記ローカル網に接続されていると判断された場合のみ、前記受信装置との間で、認証・鍵交換を実行する工程とを含むことを特徴とする送信方法。
【請求項８】　前記判断工程は、前記受信装置が、前記ローカル網に割り当てられたアドレス上に存在するか否かを検知するステップ、を含む、ことを特徴とする請求項７に記載の送信方法。
【請求項９】　前記判断工程は、前記受信装置が、送信装置と同一のローカルスコープ内に存在するか否かを検知するステップ、を含む、ことを特徴とする請求項７に記載の送信方法。
【請求項１０】　前記判断工程の後に、前記受信装置が前記ローカル網に接続されていないと判断された場合のみ、前記受信装置に認証不許可通知を送信する工程を、さらに含む、ことを特徴とする請求項７に記載の送信方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、著作権保護を実現する機能を備えた送信装置およびその送信方法に関する。
【０００２】
【従来の技術】近年の、デジタル化・ネットワーク化の進展に伴って、デジタル情報家電と呼ばれる商品が増加して来ている。デジタル情報家電は、デジタル放送の開始に伴い、普及が期待される商品群である。このデジタル情報家電には、デジタル放送対応テレビや、セットトップボックス、デジタルVTR、DVDプレーヤ、ハードディスクレコーダ等、デジタルデータ・デジタルコンテンツを扱う商品が広く含まれる。
【０００３】このようなデジタル情報家電を利用する際に、考慮すべき事柄の一つとして、著作物の著作権による保護、が挙げられる。デジタルデータは、コピー時の品質劣化がない等の利点が強調される反面、不正コピーが容易である等の欠点を持っているためである。たとえばデジタルAV機器どうしを接続するデジタルネットワークであるIEEE1394には、著作権侵害の防止のため、認証・鍵交換機構や、データ暗号化の機能が備えられる。
【０００４】ここで、著作権保護が必要なAVデータを、送信装置から受信装置に転送する場合を考える。この転送において、注意すべき点は、個人あるいは家族の楽しむ範囲内で、著作権保護の必要なAVデータのやり取りを行なうことが、著作権保護の前提である点である。そして、他人との間でのAVデータのやり取りは、視聴料や著作権料等の支払いが伴わない限り、行われるべきではないという点である。
【０００５】
【発明が解決しようとする課題】近い将来、デジタルネットワークの種類は、無線や、パソコンネットワーク等、いろいろな種類に増加するものと考えられるが、これらの多くについては、未だ著作権保護が考慮されていないのが現状である。
【０００６】また、ネットワークはローカルなものからグローバルなものまで幅広くあり、上記で説明したように、著作権保護の観点からは、明確に区別することが必要がある。
【０００７】本発明は、このような課題を解決し、受信装置がローカル網上に存在するか否かを確認することで、ローカル網上に存在する受信装置のみと認証・鍵交

換を実行できる送信装置、およびその送信方法を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記課題を解決するため、本発明は、特定の端末のみが接続可能なローカル網に接続され、暗号化されたデータを受信装置に送信する送信装置であり、受信装置に暗号化データを送信する送信部と、受信装置がローカル網に接続されているか否かを判断する判断部と、ローカル網に接続されていると判断された受信装置のみとの間で、認証・鍵交換を実行する認証・鍵交換部と、から構成される送信装置であることを第１の特徴とする。ここで、「ローカル網」とは、個人の範囲内、あるいは家族間でのデータのやりとりが行なわれる網であり、たとえばIEEE1394等のホームネットワークである。

【０００９】本発明の第１の特徴では、このローカル網内に閉じた通信のみを、個人あるいは家族間で楽しむための通信とみなすことで、著作権保護を行なうべきデータのやりとりを許容する。そして、このローカル網で閉じない通信は、個人あるいは家族間で楽しむための通信とみなすことができないため、著作権保護を行なうべきデータのやりとりを許容しない。このため、データ再生を要求する受信装置がローカル網上に存在するか否かをあらかじめ判断し、その判断結果に基づいて、受信装置と認証・鍵交換を実行することで、著作権保護を考慮したデータのやりとりが可能となる。すなわち、ローカル網に接続された受信装置のみが、認証・鍵交換を実行し、それにより、暗号化されたデータを復号できるようになる。

【００１０】本発明の第２の特徴は、上記の第１の特徴で述べた送信装置が実現する送信方法に係り、特定の端末のみが接続可能なローカル網に接続された送信装置から暗号化されたデータを受信装置に送信する送信方法であって、その受信装置からのデータ送信要求を受け取る工程と、そのデータ送信要求に基づき、受信装置に暗号化データを送信する工程と、受信装置からの認証要求を受け取る工程と、受信装置がローカル網に接続されているか否かを判断する工程と、受信装置がローカル網に接続されていると判断された場合のみ、受信装置との間で、認証・鍵交換を実行する工程と、を少なくとも含む送信方法であることである。

【００１１】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態について詳細に説明する。以下の図面の記載において、同一または類似の部分には同一または類似の符号を付している。

【００１２】図１は、本発明の実施の形態に係る送信装置が配置された、ネットワーク・システムの全体構成を示すブロック図である。図１に示すように、本発明の実施の形態に係る送信装置１０は、イーサネット（登録商標）等のローカル網１２に接続される。そして、ローカル網１２にルータ１４が接続され、ルータ１４によって、ローカル網１０とインターネット１６とが接続される。ローカル網１２には受信装置１８ａが接続され、インターネット１６には受信装置１８ｂが接続され、受信装置１８ａおよび１８ｂの両方が、送信装置１０から送信されるAVデータを受信しようとすることになる。AVデータとしてはたとえば、テキストや、写真、イラスト、絵画、アニメ、映画、音楽、音声、テレビ番組、WWWデータ等が挙げられる。ここでは、説明の簡単化を図るため、AVデータの一部に著作物が含まれる、あるいはAVデータ自体が著作物であるとする。

【００１３】ここで、送信装置１０から受信装置１８ａおよび１８ｂに、著作権保護の必要なAVデータを転送する場合を考える。この場合、注意すべき点は、従来の技術の説明でも述べたように、個人、あるいは拡大解釈して家族の楽しむ範囲内で、AVデータのやりとりを行なうことが著作権保護の前提であり、他人との間のAVデータのやりとりは、視聴料や著作権料の支払いが伴わない限り、行なわれるべきではないということである。たとえば他人との間でのデータのやりとりとしては、インターネットや電話網等の公衆網を介したオープンな通信が挙げられ、個人の範囲内、あるいは家庭間のデータのやりとりの典型例として、IEEE1394等のホームネットワークに閉じた通信が挙げられる。

【００１４】そこで、著作権保護を行なうため、図１のネットワーク・システムにおけるAVデータの転送に関し、次の２つの規則を用いる。

【００１５】（Ａ）ローカル網１２に閉じた通信は、著作権保護を行なうべきAVデータのやりとりを許容する。

【００１６】（Ｂ）ローカル網１２で閉じない通信は、著作権保護を行なうべきAVデータのやりとりを許容しない。

【００１７】ここで、上記（Ａ）の規則は、ローカル網１２で閉じた通信は、個人あるいは家庭間で楽しむための通信と見なすことができるからであり、上記（Ｂ）の規則は、ローカル網１２で閉じない通信は、個人あるいは家庭間で楽しむための通信と、通常、見なすことができないからである。

【００１８】図２は、本発明の実施の形態に係る送信装置の構成を示すブロック図である。図２に示すように、この実施の形態に係る送信装置１０は、受信装置１８（１８ａ，１８ｂ）との間での認証・鍵交換処理を実行する認証・鍵交換処理部２０と、認証・鍵交換処理を要求する受信装置１８との通信が、上記の（Ａ）および（Ｂ）の規則のいずれに該当するかを判断するローカル通信判断部２２と、暗号化されたAVデータを受信装置１８に送信する送信部２４と、ローカル網１２とのインターフェースとなるネットワークインターフェース２６と、から構成される。図２では、ローカル通信判断部２

２は、認証・鍵交換処理部２０内に配置されているが、もちろん、認証・鍵交換処理部２０外に配置されてももちろん構わない。

【００１９】次に、図３ないし図５を参照して、本発明の実施の形態に係る送信装置の動作について説明する。図３は、本発明の実施の形態に係る送信装置１０と、ローカル網１２に接続された受信装置１８ａと、の間の処理シーケンスチャートであり、図４は、本発明の実施の形態に係る送信装置１０と、インターネット１６に接続された受信装置１８ｂと、の間の処理シーケンスチャートであり、図５は、本発明の実施の形態に係る送信装置１０の送信方法の処理手順を示すフローチャートである。

【００２０】（イ）送信装置１０と受信装置１８ａとの間の通信

（１）図３のステップＳ１０１において、受信装置１８ａが、ローカル網１２を介して、送信装置１０に対して、AVデータの再生を要求する（図５のステップＳ３０１）。AVデータの再生要求は、たとえばオーディオ・ビジュアル・コントロール（AV/C）コマンドを用いて、再生要求のコマンドを発行することで、行われる。

【００２１】（２）図３のステップＳ１０２において、AVデータの送信要求を受けた送信装置１０は、著作権保護のため、暗号化鍵K1で暗号化されたAVデータを、ローカル網１２を介して、受信装置１８ａに送信する（図５のステップＳ３０２）。

【００２２】（３）図３のステップＳ１０３において、暗号化されたAVデータを受信した受信装置１８ａは、送信装置１０に対して、認証・鍵交換を要求する（図５のステップＳ３０３）。

【００２３】（４）図３のステップＳ１０４において、認証・鍵交換要求を受けた送信装置１０は、その認証・鍵交換要求のパケットに基づいて、受信装置１８ａがローカル網１２上に存在するか否かを判断する（図５のステップＳ３０４）。ローカル網１２上に存在すると判断できる基準として、たとえば次の２つが挙げられる。

【００２４】（C）認証・鍵交換要求パケットのソースアドレス、すなわち受信装置１８ａのアドレス、のサブネットIDが、送信装置１０自身のサブネットIDと一致すること。

【００２５】（D）IPv6パケットのスコープフィールドがローカルスコープを示していること。

【００２６】なお、この判断は、受信装置１８ａからの再生要求のパケットに基づいて、実行しても、もちろん構わない。また、これら再生要求のパケットおよび認証・鍵交換要求のパケットは、その転送中に、改ざん等がなされてしまうと、正確な判断を行なうことができなくなる。このため、各パケットのソースアドレスおよびスコープフィールドそれぞれの値に、改ざん検出のための署名等を施すべきである。

【００２７】（５）受信装置１８ａはローカル網１２上に存在するので（図５のステップＳ３０４ＹＥＳ）、図３のステップＳ１０５において、送信装置１０は、受信装置１８ａとの間で、認証・鍵交換を実行する（図５のステップＳ３０６）。この認証・鍵交換によって、受信装置１８ａは、暗号化ＡＶデータの復号のために必要な復号鍵を入手する。たとえば、利用される暗号技術が共通鍵暗号であれば、復号鍵は暗号化鍵K1と同一である。

【００２８】（６）図３のステップＳ１０６において、復号鍵K1を入手した受信装置１８ａは、先に受信したAVデータを復号する。

【００２９】（ロ）送信装置１０と受信装置１８ｂとの間の通信

（１）図４のステップＳ２０１において、受信装置１８ｂが、インターネット１６、ルータ１４およびローカル網１２、を介して、送信装置１０に対して、AVデータの再生を要求する（図５のステップＳ３０１）。上記（イ）の場合と同様、AVデータの再生要求は、たとえばオーディオ・ビジュアル・コントロール（AV/C）コマンドを用いて、再生要求のコマンドを発行することで、行われる。

【００３０】（２）図４のステップＳ２０２において、AVデータの送信要求を受けた送信装置１０は、著作権保護のため、暗号化鍵K1で暗号化されたAVデータを、ローカル網１２、ルータ１４およびインタネット１６を介して、受信装置１８ｂに送信する（図５のステップＳ３０２）。

【００３１】（３）図４のステップＳ２０３において、暗号化されたAVデータを受信した受信装置１８ｂは、送信装置１０に対して、認証・鍵交換を要求する（図５のステップＳ３０３）。

【００３２】（４）図４のステップＳ２０４において、認証・鍵交換要求を受けた送信装置１０は、その認証・鍵交換要求のパケットに基づいて、受信装置１０ｂがローカル網１２上に存在するか否かを判断する（図５のステップＳ３０４）。

【００３３】（５）受信装置１８ｂはローカル網１２上に存在しないので（図５のステップＳ３０４ＮＯ）、図４のステップＳ２０５において、送信装置１０は、受信装置１８ｂに対して、認証不許可を通知する（図５のステップＳ３０５）。この認証不許可によって、受信装置１８ｂは、先に受信したAVデータを復号するために必要な復号鍵を入手することができない。このため、ローカル網１２上に存在しない受信装置１８ｂが、不正にAVデータを入手することを、未然に防ぐことが可能となる。

【００３４】このように、本発明の実施の形態によれば、ローカル網上に存在する受信装置のみに対して、著作権保護の必要なAVデータを送信することが可能となる。このため、近年のデジタル化・ネットワーク化に伴って増加する一方である、ネットワーク上で送信される

著作物を適切に保護することが可能となり、その重要性はきわめて高いものである。

【００３５】

【発明の効果】本発明によれば、受信装置がローカル網上に存在するか否かを確認することで、ローカル網上に存在する受信装置のみと認証・鍵交換を実行する送信装置を実現できる。

【００３６】本発明によれば、受信装置がローカル網上に存在するか否かを確認することで、ローカル網上に存在する受信装置のみと認証・鍵交換を実行する送信方法を実現できる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る送信装置が配置された、ネットワーク・システムの全体構成を示すブロック図である。

【図２】本発明の実施の形態に係る送信装置の具体的な構成を示すブロック図である。

【図３】本発明の実施の形態に係る送信装置と受信装置間の処理シーケンスチャートである。

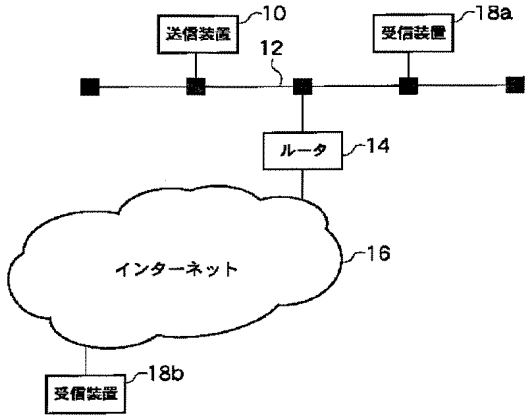
【図４】本発明の実施の形態に係る送信装置と受信装置間の処理シーケンスチャートである。

【図５】本発明の実施の形態に係る送信装置の送信方法の処理手順を示すフローチャートである。

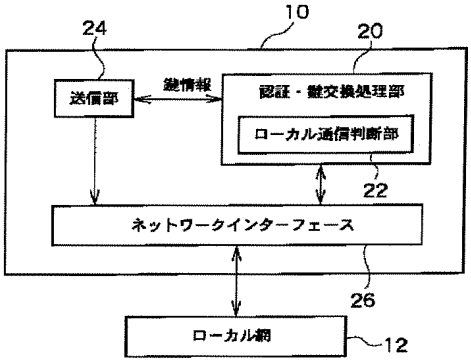
【符号の説明】

１０　送信装置
１２　ローカル網
１４　ルータ
１６　インターネット
１８　受信装置
２０　認証・鍵交換処理部
２２　ローカル通信判断部
２４　送信部
２６　ネットワークインターフェース

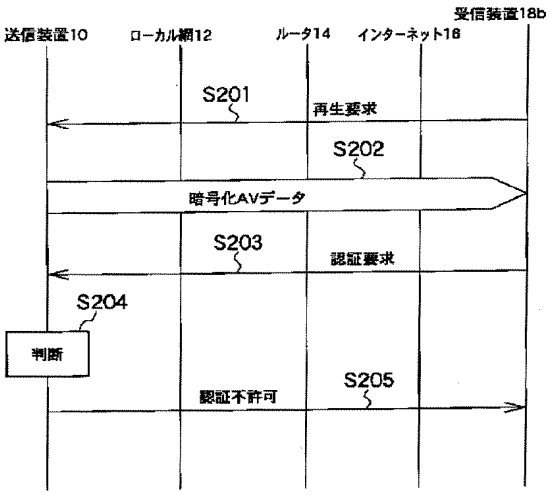
【図１】



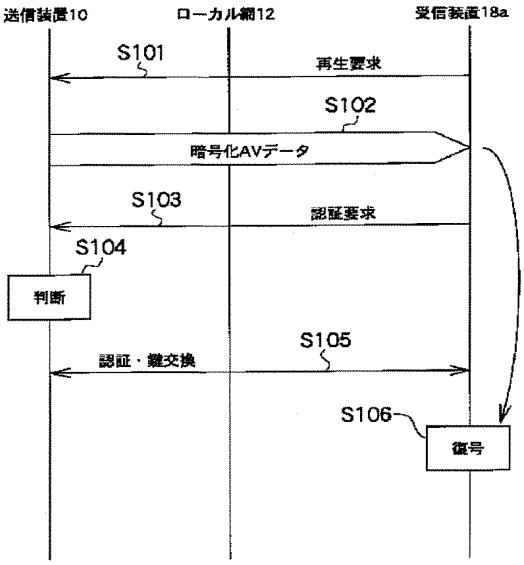
【図２】



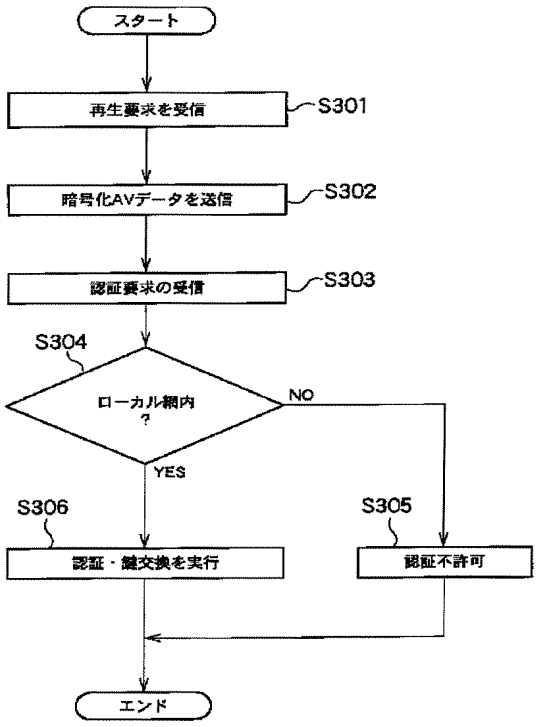
【図４】



【図３】



【図５】



フロントページの続き

Ｆターム(参考)　5B017 AA03 BA05 BA07 CA16
5J104 AA07 AA12 AA16 EA04 EA15
KA02 PA07
5K030 GA15 HA08 HB21 HC14 JL09
JT04 LD20
5K033 AA08 BA01 BA15 CB01 DA01
DA13